Information Sheet for preparing an Information Disclosure Statement under Rule 1.56

Suzuye Ref.03S0936

Foreign Patent Documents

Document No.: 2000-76402, published March 14, 2000

Country: Japan

Copy of reference: attached

Language: non-English

English translation: not attached for it is not readily available

Concise Explanation of Pertinency: This publication is referred to in the specification. See page 2, line 7.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－76402
（P2000－76402A）
(43)公開日　平成12年３月14日(2000.3.14)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　19/00	Ｐ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｃ	５Ｂ０３５
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｅ	５Ｂ０５８

審査請求　未請求　請求項の数３　ＯＬ　（全４頁）

(21)出願番号　特願平10－243071

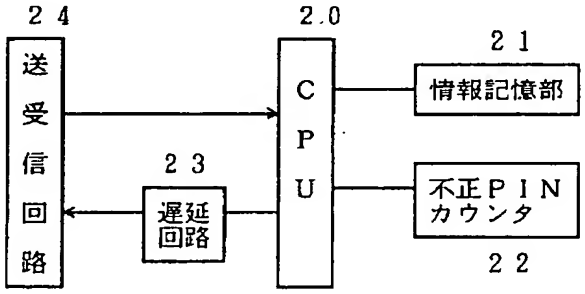
(22)出願日　平成10年８月28日(1998.8.28)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　矢野義博
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内
(72)発明者　半田富己男
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内
(74)代理人　100092495
弁理士　蛭川　昌信　（外７名）

最終頁に続く

(54)【発明の名称】　レスポンスタイムを可変化したＩＣカード

(57)【要約】
【課題】　総当たり攻撃からＰＩＮの類推を不可能にし、セキュリティを向上させる。
【解決手段】　情報記録手段２１と情報処理制御手段２０とを持ち、情報処理制御手段２０により外部から入力された命令を解釈し、情報記録手段２１にアクセスして一定の処理を行ってレスポンスを返すＩＣカードにおいて、前記レスポンスのタイミングを遅延させる遅延手段２３を設けたものである。



1

【特許請求の範囲】
【請求項１】　情報記録手段と情報処理制御手段とを持ち、前記情報処理制御手段により外部から入力された命令を解釈し、情報記録手段にアクセスして一定の処理を行ってレスポンスを返すＩＣカードにおいて、前記レスポンスのタイミングを遅延させる遅延手段を設けたことを特徴とするレスポンスタイムを可変化したＩＣカード。
【請求項２】　利用者コードの照合命令、または認証コードの認証命令が連続し、所定回数に達したことを条件に前記遅延手段によりレスポンスを遅延させるようにしたことを特徴とする請求項１記載のレスポンスタイムを可変化したＩＣカード。
【請求項３】　前記遅延手段は、照合命令または認証命令の回数が所定値に達する毎に階段状に遅延時間を増大させることを特徴とする請求項２記載のレスポンスタイムを可変化したＩＣカード。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はＩＣカードと端末装置間の通信において、端末装置より入力される命令に対するＩＣカードからのレスポンスの送信タイミングを可変化するようにしたＩＣカードに関する。
【０００２】
【従来の技術】従来、ＩＣカードの不正利用に対する防止策として外部からの命令に対するＩＣカードのレスポンス時間に着目したものが知られている。例えば、特開昭６２―２５１９６３号公報は、Ｐｅｒｓｏｎａｌ　ＩｄｅｎｔｉｆｉｃａｔｉｏｎＮｕｍｂｅｒ（以下ＰＩＮ）の照合のためのレスポンス時間をあえて一定にするもので、これはＰＩＮが正しいか、間違っているかを判断するとき、判断するロジックが変わるとレスポンス時間が変化し、そのためロジックの類推が可能となるので、あえてレスポンス時間を一定にすることで、悪意のある者からのロジッの類推を防ぐように工夫したものである。
【０００３】また、特開平１０―６９２２２号公報では、ＩＣカード内で暗号化処理、復号処理を行うものにおいて、暗号化のために使用した鍵とレスポンス時間とが相関をもち、レスポンス時間から鍵の性質が分かる可能性があるため、レスポンス時間をランダムに遅延させることにより鍵の類推を防止している。
【０００４】
【発明が解決しようとする課題】ＩＣカードの情報記録部あるいはアクセス制御部へのアクセスのためのコマンドに対するＩＣカードからのレスポンスのタイミングは、照合や認証の正否等の結果や、レスポンスに載せる情報生成手順によって異なるが、同じ処理手順で行う場合、処理に要する時間はほぼ一定になる傾向がある。例えば、ＩＣカードのような高セキュリティな機能を有する媒体において、不正な利用者によるランダムなＰＩＮ入力に対しても照合結果の出力に要する時間は正当な利用者のものと変わらず、そのため総当たり攻撃によってＰＩＮが分かってしまう可能性がある。

2

【０００５】本発明は上記課題を解決するためのもので、総当たり攻撃からＰＩＮや認証用暗号鍵の類推を不可能にし、セキュリティを向上させることを目的とする。
【０００６】
【課題を解決するための手段】本発明は、情報記録手段と情報処理制御手段とを持ち、前記情報処理制御手段により外部から入力された命令を解釈し、情報記録手段にアクセスして一定の処理を行ってレスポンスを返すＩＣカードにおいて、前記レスポンスのタイミングを遅延させる遅延手段を設けたことを特徴とする。また本発明は、利用者コードの照合命令または認証コードの認証命令が連続し、所定回数に達したことを条件に遅延手段によりレスポンスを遅延させるようにしたことを特徴とする。また本発明は、遅延手段は、照合命令または認証命令の回数が所定値に達する毎に階段状に遅延時間を増大させることを特徴とする。
【０００７】
【発明の実施の形態】以下、本発明の実施の形態について説明する。図１は本発明のシステム概念図で、端末装置１に対してＩＣカード２をセットすると、端末装置１からはＩＣカード２に対して、コマンド（命令）を送信し、これを受信したＩＣカード２はコマンドを解釈して書き込み、読み取り、読み出し等の処理を実行し、処理結果をレスポンスとして端末装置１に返すようになっている。
【０００８】図２は本発明のＩＣカードの構成を示す概念図である。ＩＣカードにはＣＰＵ２０、情報記憶部２１、不正ＰＩＮカウンタ２２、遅延回路２３、送受信回路２４を有している。情報記憶部２１はプログラム記憶領域、作業エリア、書換え可能な不揮発性メモリ領域を有している。ＣＰＵ２０は、端末装置１から送信されるコマンドを受信するとコマンドと共に送信されたデータを読み込み、情報記憶部２１にアクセスして必要な処理を行い、結果を送受信回路２４よりレスポンスとして出力する。さらに本発明においては、不正ＰＩＮカウンタ２２、遅延回路２３を有している。不正ＰＩＮカウンタ２２は連続してＰＩＮ入力が行われたとき、その入力された回数をカウントするものであり、遅延回路２３はレスポンス時間を遅延させるためのものである。遅延手段は、遅延回路ではソフトウエアによる実現のいずれでもよい。
【０００９】図３はＩＣカードの信号の流れを示しており、図示するように、送受信回路２４を通してＰＩＮ入力が行われると、ＣＰＵ２０では入力したＰＩＮが真正か否かを判定するための照合を行い、正否を送受信回路

3

２４を通してレスポンスとして送信する。不正ＰＩＮカウンタ２２は連続して入力される不正なＰＩＮ入力回数をカウントし、例えば、図４に示すように、不正ＰＩＮ入力回数が所定値に達すると、所定の遅延時間を遅延回路２３に設定する。この不正ＰＩＮ入力回数に対して階段状に遅延時間が増えるように設定する。このため、総当たり攻撃でＰＩＮ入力を行おうとすると、入力回数に応じて応答時間が飛躍的にかかってしまうため、結局は真正なＰＩＮ情報を盗み取ることは不可能である。

【００１０】図５はレスポンスを遅延させる処理フローを示す図である。ＰＩＮ入力があってこれを受信すると（Ｓ１）、入力されたＰＩＮが真正か否か判断するための照合を行う（Ｓ２）。照合の結果、真正なものであれば次の処理に進み、真正でないと判断されると不正ＰＩＮカウンタをインクリメントする（Ｓ３、Ｓ４）。次いで、不正ＰＩＮカウンタの値が所定値Ｋ以上か否か判断し（Ｓ５）、所定値Ｋ未満であれば、通常のタイミングでＰＩＮが間違っていることをレスポンスとして出力し（Ｓ７）、所定値Ｋ以上であればレスポンスの時間を遅

4

*延させ（Ｓ６）、出力する。

【００１１】

【発明の効果】以上のように本発明によれば、連続的に入力される不正なＰＩＮ入力に対し、ＩＣカードからのレスポンス送信までの時間を大幅に遅らせることによりランダムなＰＩＮ入力による総当たり攻撃を防ぐことが可能となる。

【図面の簡単な説明】

【図１】　本発明のシステム概念図である。

【図２】　本発明のＩＣカードの構成を示す図である。

【図３】　ＩＣカードの信号の流れを示す図である。

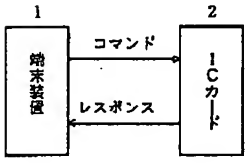
【図４】　不正ＰＩＮ入力回数に対する遅延時間の関係を示す図である。

【図５】　レスポンスを遅延させる処理フローを示す図である。

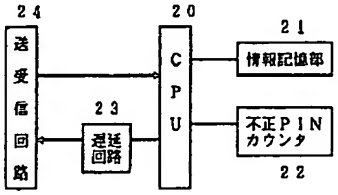
【符号の説明】

１…端末装置、２…ＩＣカード、２０…ＣＰＵ、２１…情報記憶部、２２…不正ＰＩＮカウンタ、２３…遅延回路、２４…送受信回路。

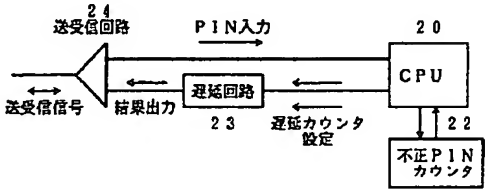
【図１】



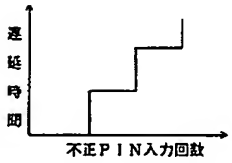
【図２】



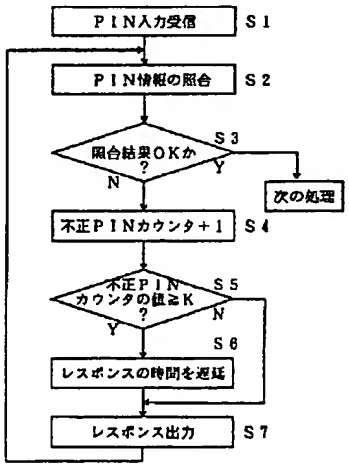
【図３】



【図４】



【図５】



フロントページの続き

(72)発明者　松田雅之
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内

(72)発明者　柴田直人
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内

Ｆターム(参考)　5B017 AA01 BA05 BB02 BB03 BB10 CA14
5B035 AA14 BB09 CA12
5B058 CA27 KA33